

I hereby certify that this correspondence is being filed via
EFS-Web with the United States Patent and Trademark Office
on September 4, 2003

TOWNSEND and TOWNSEND and CREW LLP

By: 
Andrea S. Beck

PATENT
Attorney Docket No. 016222-012810US
Client Ref. No.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Sonia Reed

Application No.: 10/656,858

Filed: September 5, 2003

For: METHOD AND SYSTEM FOR
FACILITATING DATA ACCESS AND
MANAGEMENT ON A SECURE
TOKEN

Confirmation No. 8576

Examiner: Mahesh H. Dwivedi

Technology Center/Art Unit: 2168

APPELLANTS' BRIEF UNDER
37 CFR §41.37

Mail Stop Appeal Brief
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Further to the Notice of Appeal submitted on October 5, 2007 for the above-referenced application, Appellants submit this Appellants' Brief pursuant to 37 C.F.R. §41.37. The Commissioner is authorized to deduct the fee of \$500.00 pursuant to 37 C.F.R. §41.20(b)(2) from deposit account number 20-1430 and any additional fees associated with this Brief.

1. REAL PARTY IN INTEREST

The real party in interest of the subject patent application is Visa International Service Association, the assignee of the application.

2. RELATED APPEALS AND INTERFERENCES

There are no related appeals and interferences.

3. STATUS OF CLAIMS

An Amendment After Final canceling claims 1-2, 14, 16-17, and 19 is being filed concurrently herewith. After entry of the Amendment After Final, claims 13, 20-21, 23-28, 30-33, 35-40, 42-52 and 54-61 would be pending and finally rejected. Appellants appeal from the rejection of all pending claims.

4. STATUS OF AMENDMENTS

An Amendment After Final is being filed concurrently herewith. Appellants believe that the Amendment After Final will be entered as it only cancels claims and reduces the issues for appeal.

5. SUMMARY OF CLAIMED SUBJECT MATTER

In the following summary, Appellants have provided exemplary references to sections of the specification and drawings supporting the subject matter defined in the claims as required by 367 C.F.R. §41.37. The specification and drawings also include additional support for other exemplary embodiments encompassed by the claimed subject matter. Thus, these references are only intended to be illustrative and not restrictive.

Current technologies now allow multiple applications to be implemented on a single chip card. This ability to have multiple applications on a chip card has been identified as one of the key components for enhancing the business case of a chip card program. These multiple applications include, for example, value-add programs and the associated data required to operate them successfully. From a business perspective, it is preferable that value be obtained

for all parties involved in the chip card program, including the issuer, acquirer, application owner, value add service provider and the cardholder.

It is desirable to provide value-add applications on the chip card to provide for the ability to maximize and efficiently use available space on the chip card to allow multiple applications or programs to operate, and to deploy an acceptance infrastructure that allows consumers to take full advantage of the functionality provided by the chip card.

While it is now possible to implement multiple applications on a chip card, these multiple applications (and their associated data) are often kept independent of one another within the chip card. For example, data belonging to one application is not shared by another application within the chip card, which in some cases result in redundancy. Due to the limited size of the chip card, such redundancy adversely affects the optimal use of resources on the chip card.

Embodiments of the invention include a method and a system for facilitating data access and management on a smart card. According to one exemplary embodiment, the smart card includes a storage architecture that allows data stored thereon to be shared by multiple parties. Access to data stored on the smart card is controlled by various access methods depending on the actions to be taken with respect to the data to be accessed.

According to one exemplary embodiment, the storage architecture provides a file structure that can have separate instances of the file structure. A separate instance is referred to as an environment. In one instance, an environment includes the common commands applet providing access to a directory, one or more cell groups under the directory (with each cell group being a sub-directory), and one or more cells under each cell group. Attributes and access conditions can be set at different levels including, for example, at the directory level, the cell group (or sub-directory) level and the cell level. This allows varying access levels for different parties thereby permitting data to be shared in various manners.

An embodiment of the invention allows sharing of information between multiple parties including, for example, an issuer, a merchant and a third-party sponsor such as a credit card service association. The issuer, the merchant and the third-party sponsor may be involved

in a joint loyalty program. Each of these parties may store its information on a smart card issued to a cardholder.

The information stored by these parties on the smart card can be shared in a number of ways. In one instance, the issuer may allow both the merchant and the third party sponsor to access one portion of its information stored on the smart card; in another instance, the issuer may allow only the third party sponsor to access another portion of its information while denying access to the merchant. Furthermore, access to the information can be controlled based on different access methods depending on actions to be taken with respect to the information to be accessed.

The storage architecture is flexible as to which keys are used to access files and how they are used. Keys can be stored in key files with an attached key index referenced internally from the various files to be protected. This means, for instance, that the same file can be protected by different keys that relate to different commands (e.g. one key for read, another key for update) or that multiple files can be protected by the same key for all commands.

In an exemplary embodiment, two sets of keys can be used. One set is used for transferring ownership of card-space from the issuer or its delegate to the value add service provider or its delegate. The other set is used by the value add service provider to access specific cells. These keys control access to cells and authentication of specific cell data.

As described above, embodiments of the present invention provide for a set of functions and a repository for data that allow multiple parties with existing business relationships to access and share chip card data according to agreed security controls.

Embodiments of the invention may be illustrated by the various independent and dependent claims described below.

Independent claim 13

Claim 13 is directed to a system for facilitating data management on a secure token. The system comprises a client having a plurality of applications residing thereon and a secured token having a storage architecture (paragraphs [0015]-[0028], and [0030]). The storage architecture includes: a directory, one or more cell groups under the directory, and one or more

cells under each cell group. The directory has one or more attributes that are used to control access to the directory by the plurality of applications (paragraph [0020]). Each cell group has one or more associated attributes used to control access to that cell group by the plurality of applications (paragraph [0029]). Each cell has one or more associated attributes used to control access to that cell by the plurality of applications (paragraph [0035]). The attributes associated with each cell permit a first set of operations on the contents of that cell by a first application and a second set of operations on the contents of that cell by a second application (paragraphs [0017] and [0042]). The first set of operations is different from the second set of operations (paragraphs [0017] and [0042]). The attributes associated with the directory, cell group, or cell are associated with a passcode or a key that the client is adapted to use to access data in the directory, cell group or cell (paragraphs [0038]-[0039] and [0049]).

Independent claim 18

Claim 18 is directed to a system for facilitating data management on a secure token. The system includes a client having a plurality of applications residing thereon, and a secure token having a storage architecture (paragraphs [0015]-[0028] and [0030]). The storage architecture includes a directory and one or more attributes associated with the directory, wherein the one or more attributes associated with the directory are used to control access to the directory by the plurality of applications (paragraph [0020]), one or more cell groups under the directory, each cell group having one or more associated attributes, wherein the one or more attributes associated with a cell group are used to control access to that cell group by the plurality of applications (paragraph [0029]), and one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications (paragraph [0017]), wherein the secure token is a smart card. The smart card is an open platform smart card (paragraph [0019]). The one or more attributes are associated with the directory, cell group, or cell are associated with a passcode or a key, wherein the client is adapted to use the passcode or key to access data in the directory, cell group, or cell (paragraphs [0038], [0039], and [0049]).

Independent claim 20

Claim 20 is directed to a secure token. The secure token includes a directory and one or more attributes associated with the directory, wherein the one or more attributes associated with the directory are used to control access to the directory by a plurality of applications associated with a client (paragraphs [0015]-[0028] and [0030]). The secure token also includes one or more cell groups under the directory, each cell groups having one or more associated attributes, wherein the one or more attributes associated with a cell group are used to control access to that cell group by the plurality of applications and one or more cells under each cell group, each cell having one or more associated attributes used to control access to that cell by the plurality of applications (paragraphs [0028]-[0029]). The attributes associated with the cell group allow applications access to a cell group depending on the access condition that is met. If a first access condition is satisfied, a first application is permitted access to the cell group and if a second access condition is satisfied, a second application is permitted access to the cell group (paragraph [0029]). The first and second access conditions are different from one another. Each attribute associated with the directory, cell group, or cell is associated with a passcode or key, wherein the client is adapted to use the passcode or key to access data in the directory, cell group or cell (paragraph [0029]).

Independent claim 32

Claim 32 is directed to a secure token. The secure token includes a directory and one or more attributes associated with the directory, (paragraph [0028]) that are used to control access to the directory by the plurality of applications associated with a client terminal, (paragraph [0028]). The secure token also includes one or more cell groups under the directory (paragraph [0028]), each cell group has one or more associated attributes (paragraph [0029]), wherein the one or more attributes associated with a cell group are used to control access to that cell group by the plurality of applications (paragraph [0029]). Additionally, the secure token has one or more cells under each cell group (paragraph [0030]), each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications (paragraph [0035]). The attributes associated

with each cell permit a first set of operations on the contents of that cell by a first application, wherein the attributes associated with the cell permit a second set of operations on the contents of that cell by a second application (paragraph [0030]). The first set of operations is different from the second set of operations and the one or more attributes associated with the directory, cell group, or cell are associated with a passcode or a key, wherein the client is adapted to use the passcode or key to access data in the directory, cell group or cell (paragraph [0029]).

Independent claim 37

Claim 37 is directed to a secure token. The secure token includes a directory and one or more attributes associated with the directory, (paragraph [0020]) wherein the one or more attributes associated with the directory are used to control access to the directory by the plurality of applications associated with a client (paragraph [0020]). The secure token also includes one or more cell groups under the directory (paragraph [0028]), each cell group having one or more associated attributes (paragraph [0029]), wherein the one or more attributes associated with a cell group are used to control access to that cell group by the plurality of applications (paragraph [0029]). Additionally, the secure token includes one or more cells under each cell group (paragraph [0030]), each cell having one or more associated attributes, wherein the attributes associated with a cell are used to control access to that cell by the plurality of applications (paragraph [0035]). The secure token is an open platform smart card (paragraph [0019]). The attributes associated with the directory, cell group, or cell are associated with a passcode or a key, wherein the client is adapted to use the passcode or key to access data in the directory, cell group or cell (paragraph [0029]).

Independent claim 39

Claim 39 is directed to a method for facilitating data management on a secure token. The method comprises the step of providing a directory (paragraph [0016]) and attributes associated with the directory (paragraph [0034]), wherein the attributes are used to control access to the directory by applications associated with a client (paragraphs [0034]). The method further comprises one or more cell groups under the directory (paragraph [0028]), each group has

associated attributes that are used to control access that cell group by a plurality of applications (paragraph [0028]). Each cell group has one or more cells with associated attributes used to control access to that cell (paragraph [0030]). The attributes associated with the cell groups permit access to one or more applications based on whether certain access conditions are met. Different access conditions permit different applications access to the cell groups (paragraph [0029]). The attributes associated with the directory, cell group, or cell are further associated with a passcode or key that is used by the client to access data in the directory, cell group or cell (paragraph [0029]).

Independent claim 56

Independent claim 56 is directed to a method for facilitating data management on a secure token (paragraphs [0015]-[0028] and [0030]). The method includes providing a directory and one or more attributes associated with the directory, wherein the one or more attributes associated with the directory are used to control access to the directory by a plurality of applications associated with a client (paragraph [0029]). It also includes providing one or more cell groups under the directory, each cell group having one or more associated attributes, wherein the one or more attributes associated with a cell group are used to control access to that cell group by the plurality of applications, and providing one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications (paragraph [0035]). The secured token is a smart card, and is an open platform smart card (paragraph [0019]). One or more attributes are associated with the directory, cell group, or cell and are associated with a passcode or a key (paragraph [0038] and [0039]). The client is adapted to use the passcode or key to access data in the directory, cell group, or cell (paragraphs [0038] and [0039]).

Dependent claim 58

Claim 58 depends on claim 39 and additionally recites "wherein the first application is associated with a first party and the second application is associated with a second

party, and wherein the first party and the second party have an existing business relationship and agree to share data on the secure token according to agreed security controls." (Paragraph [0072].)

Dependent claim 59

Claim 59 depends from claim 58 and additionally recites "wherein the first application or the second application is a loyalty application." (Paragraph [0074]).

Dependent claim 60

Claim 60 depends from claim 60 and additionally recites the phrase "wherein the first application can access only that cell group while the second application can access that cell group and additional cell groups." (Paragraph [0074].)

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

In the final Office Action mailed June 6, 2007, claim 1-2 and 4-12 were rejected under 35 U.S.C. §112 as being indefinite. As noted above, Appellants are filing an Amendment After Final with this Brief. The Amendment After Final cancels the rejected claims 1-2 and 4-12 (along with claims 14, 16, 17, and 19), so the rejection under §112 should be moot.

Thus, the rejections to be reviewed on appeal are:

Claims 13, 20-21, 23-28, 30-33, 35-36, 38-40, 42-52, 54-55, and 57-61 are rejected as obvious under 35 U.S.C. §103(a) over Deo et al. (U.S. Patent No. 6,970,891) and Carlisle et al. (U.S. Patent No. 5,649,118); and

Claims 37 and 56 are rejected as obvious over Deo et al., Carlisle et al., and Brittenham et al. (U.S. Patent No. 6,880,084).

For purposes of this appeal, Appellants would like to separately argue the patentability of independent claims 13 and 39 and dependent claims 58, 59, and 60. Claims 20-21, 23-28, 30-33, 35-36, 38, and 61 may stand or fall with respect to claim 13, and claims 40, 42-52, and 54-57 may stand or fall with respect to independent claim 39. No admissions are made

by the groupings of claims, and Appellants reserve the right to pursue features in any of the claims in continuation applications.

7. ARGUMENT

A. Rejection of claims 13, 20-21, 23-28, 30-33, 35-36, 38-40, 42-52, 54-55, and 57-61 under 35 U.S.C. 103(a) as being obvious over Deo et al. and Carlisle et al.

At page 3 of the final Office Action, claims 1-2, 4-14, 16-17, 19-21, 23-28, 30-33, 35-36, 38-40, 42-52, 54-55, and 57 are rejected as obvious over Deo et al. and Carlisle et al. The Examiner alleges that Deo et al. teaches all limitations except "a directory and one or more attributes associated with the directory," "one or more cell groups under the directory each cell group having one or more associated attributes," "one or more attributes associated with the directory, cell group, or cell are associated with a passcode or key," and a "client terminal [that] is adapted to use the passcode or key to access data in the directory, cell group, or cell." See page 5 of the final Office Action.

The Examiner relies on Carlisle et al. to supplement the deficiencies of Deo et al.

1. Independent Claims 13 and 39

a. *Obviousness has not been established, since each and every element of the claims is not taught or suggested by Deo et al. and Carlisle et al.*

Obviousness has not been established, since each and every element of the claims is not taught or suggested by Deo et al. and Carlisle et al. To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). Here, neither Deo et al. nor Carlisle et al. teaches or suggests "a client having a plurality of applications residing thereon" as in independent claim 13. Independent claim 39 recites a similar limitation. At page 3 of the final Office Action, the Examiner relies on column 3, lines 44-54 of Deo et al. to teach "a client having a plurality of applications residing thereon."

Contrary to the Examiner's allegation, Deo et al. does not teach "a client having a plurality of applications residing thereon." Column 3, lines 44-54 of Deo et al. is reproduced below:

The operating system 114 includes a file system 118 that manages files stored on the smart card. Typically, smart card files are stored in nonvolatile memory, such as nonvolatile data files 120 in EEPROM 110. However, with this system, data in volatile memory may also be stored in special files, as represented by volatile data files 122 in RAM 106. The volatile files 122 make it possible for multiple resident applications 112, as well as nonresident applications 116 that are downloaded for a particular session, to share the same data in volatile memory 106 (assuming the applications are authorized).

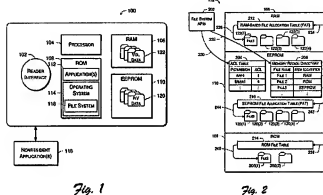
While the passage cited by the Examiner mentions "nonresident applications," such nonresident applications are "downloaded" to the memory 106 in a smartcard. The passage cited by the Examiner does not state or suggest that there is any "client" having a plurality of applications residing thereon. Deo et al.'s smart card cannot be the "client", since Deo et al.'s smart card is allegedly a "secure token." Consequently, obviousness has not been established for this reason alone.

b. Obviousness has not been established, since the modifying Deo et al. in the manner proposed by the Examiner would be contrary to the intended purpose of Deo et al.'s smartcard subsystem.

Obviousness has not been established, since the modifying Deo et al. in the manner proposed by the Examiner would be contrary to the intended purpose of Deo et al.'s smartcard subsystem. Deo et al. fails to teach or suggest at least the following limitation from independent 13: "wherein the one or more attributes associated with the directory, cell group, or cell are associated with a passcode or a key, wherein the client is adapted to use the passcode or key to access data in the directory, cell group, or cell." Independent claim 39 recites a similar limitation.

Referring to FIGS. 1 and 2 from Deo et al. below, and col. 3, line 63 to col. 4, line 13, Deo et al. uses access control mechanisms (e.g., an access control list or ACL) in a file

system 118 on an IC module 100 embodied as a smartcard (col. 3, line 17) to enforce levels of security for access to volatile files 122.



Passcodes and keys are not taught, suggested, or desired in Deo et al.

Contrary to the Examiner's allegation, there is also no reason to modify Deo et al. to include passcodes or keys. As explained by both the MPEP and the Court of Appeals for the Federal Circuit:

If a proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification.
In re Gordon, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984).
 MPEP 2143.01.

If one were to modify Deo et al. to include passcodes and keys as alleged by the Examiner, this would render an essential part of Deo et al.'s system (i.e., the file system 118 and its associated access control mechanism) obsolete. As explained at col. 3, line 44 to col. 4, line 7 of Deo et al., the file system 118 is essential to the operation of Deo et al.'s smartcard and resides inside of the smartcard. If one were to modify Deo et al. to include a client with a plurality of applications and that uses passcodes or keys to access data on a secure token, there would be no need for Deo et al.'s file system 118 and its access control mechanism, since access to directories, cell groups, and cells would already be restricted. Consequently, there is no reason to modify Deo et al. to

arrive at the pending claims, since doing so would be contrary to the intended purpose of Deo et al.'s proposed invention.

In response to this argument, the Examiner provided the following response on page 41 of the final Office Action:

In this case, Carlisle teaches [the limitation wherein the one or more attributes associated with the directory, cell group, or cell are associated with a passcode or a key, wherein the client is adapted to use the passcode or key to access data in the directory, cell group or cell of the] independent claims, and the motivation is found within Carlisle to do so (see **"access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card,"** as noted by Carlisle (Column 1, line 59-23). (Emphasis added.)

Appellants submit that the Examiner's response does not address Appellant's argument that one would not have modified Deo et al. with the teachings in Carlisle et al., because doing so would have rendered Deo et al.'s proposed invention unsatisfactory for its intended purpose. Furthermore, Deo et al. does not state or suggest that Deo et al.'s access control mechanism is deficient in any way, so it is unclear why one skilled in the art would have modified Deo et al.'s system with passcodes or keys as alleged by the Examiner. Accordingly, Appellants maintain that one would not have been led to modify Deo et al. in the manner proposed by the Examiner and that obviousness has not been established.

c. Obviousness has not been established, since the Examiner's proposed reason to combine is not in the prior art.

Obviousness has not been established, since the Examiner's proposed reason to combine is not in the prior art. As explained by the Court of Appeals for the Federal Circuit and the MPEP,

The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the

prior art, and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). MPEP 2142

Here, the Examiner alleges that one would have modified Deo et al. with passwords or keys to provide "access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by Carlisle (Column 1, lines 59-62)." Column 1, lines 59-62, of Carlisle et al. state:

In this manner, prior art systems create a commercial conflict between competitive services, which fosters a desire by some providers to restrict access by their customers to competing services.

Contrary to the Examiner's allegation, column 1, lines 59-62 does not state that passcodes and keys are necessary to provide access control at "higher" hierarchical levels. In fact, contrary to the Examiner's allegation, Carlisle et al. actually teaches away from providing access control at "higher" hierarchical levels. Carlisle et al. describes a variation on a UNIX operating system that restricts access to directories under the root directory to specific users. In this way, the control of each directory is provided to lower hierarchical levels, and not higher hierarchical levels as the Examiner alleges.

3. Dependent claim 58

Dependent claim 58 depends from independent claim 39. Dependent claim 58 specifically recites "wherein the first application is associated with a first party and the second application is associated with a second party, and wherein the first party and the second party have an existing business relationship and agree to share data on the secure token according to agreed security controls."

- a. *Obviousness has not been established, since all limitations are not taught or suggested by the cited art.*

Appellants submit that dependent claim 58 is patentable, since it depends from independent claim 39, which is patentable for the reasons provided above.

In addition, dependent claim 58 recites "wherein the first application is associated with a first party and the second application is associated with a second party, and wherein the first party and the second party have an existing business relationship and agree to share data on the secure token according to agreed security controls." Neither Deo et al. nor Carlisle et al. teaches or suggests this limitation. At page 29 of the final Office Action, the Examiner relies on the passage at column 16, lines 66-67 to column 17, lines 1-19 of Carlisle et al. Column 16, lines 66-67 to column 17, lines 1-19 of Carlisle et al. state:

Cooperation Between Service Providers

It is quite possible for service providers to form cooperative alliances. Such alliances can specify various activities which are carried out in the smart cards whenever the smart card is accessed, or when the smart card is accessed by a particular user. The number of such possibilities is limitless, and the example below is merely illustrative.

Assume, for example, that company A employs traveling salespeople who frequently need to purchase gasoline. A is likely to contract with O to issue a smart card for each of the salespeople (Holders) and request O to install A as a service provider and G as the gasoline provider. Sometime later, A may reach an agreement with bank B as a Provider of credit for the salespeople. That service can be remotely installed into all of the smart cards belonging to the salespeople by, for example, obtaining the cooperation of G.

Specifically, A can request G to install a request for communication with O whenever a smart card interacts with G and found to have A as a user but not B as a user. All that G needs to do is modify the file that is executed when H logs in to communicate with G and direct the smart card to call O.

Although this passage might suggest an "agreement" between two parties, Appellants submit that this passage does not describe an agreement to "share security controls." The word "security" is not remotely suggested in the cited passage. At best, the passage cited by

the Examiner describes allowing a gasoline provider G to install an application on a smartcard, and allowing a bank B to be a provider of credit for gas sales to employees of A. There is no mention of suggestion of an agreement between any of the parties A, G, or B to "share security controls." Since each and every limitation of claim 58 is not taught or suggested by the cited art, obviousness has not been established.

- b. Obviousness has not been established, since the reason to modify Deo et al. with an "agreement to share security controls" does not have any rational underpinning.*

Obviousness has not been established, since the reason to modify Deo et al. with an "agreement to share security controls" does not have any rational underpinning. As explained by the PTO's own "Examination Guidelines for Determining Obviousness Under 35 U.S.C. 103 in View of the Supreme Court Decision in KSR International Co. v. Teleflex" at pages 57528 and 57529 (Federal Register/Vol. 72, No. 195), "[R]ejections based on obviousness cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." Here, the Examiner alleges that one would have modified Deo et al. with passwords or keys to provide Deo et al. with "access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by Carlisle (Column 1, lines 59-62)."
As explained above, this alleged reason or motivation is not even suggested by Carlisle et al., and the rejection should be withdrawn for this reason alone.

Further, one would not have modified Deo et al. with an "agreement to share security controls" in order to provide "access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card," as alleged by the Examiner, since an "agree[ment] to share data on the secure token according to agreed security controls" would not necessarily benefit from providing access control at higher hierarchical levels. Actually, an "agreement to share security controls" allows additional access and does not further restrict access, so the Examiner's cited motivation of providing access

control at higher hierarchical levels actually teaches away from the modification proposed by the Examiner.

4. Dependent claim 59

Dependent claim 59 depends from dependent claim 58, and independent claim 39. Dependent claim 58 recites "wherein the first application or the second application is a loyalty application."

- a. Obviousness has not been established, since all limitations are not taught or suggested by the cited art.*

Appellants submit that dependent claim 59 is patentable, since it depends from independent claim 39 and dependent claim 58, which are patentable for the reasons provided above. In addition, dependent claim 59 recites "wherein the first application or the second application is a loyalty application." Neither Deo et al. nor Carlisle et al. teaches or suggests this feature. At pages 30-31 of the final Office Action, the Examiner relies on the passage at column 16, lines 66-67 to column 17, lines 1-19 of Carlisle et al. Column 16, lines 66-67 to column 17, lines 1-19 of Carlisle et al. state:

Cooperation Between Service Providers

It is quite possible for service providers to form cooperative alliances. Such alliances can specify various activities which are carried out in the smart cards whenever the smart card is accessed, or when the smart card is accessed by a particular user. The number of such possibilities is limitless, and the example below is merely illustrative.

Assume, for example, that company A employs traveling salespeople who frequently need to purchase gasoline. A is likely to contract with O to issue a smart card for each of the salespeople (Holders) and request O to install A as a service provider and G as the gasoline provider. Sometime later, A may reach an agreement with bank B as a Provider of credit for the salespeople. That service can be remotely installed into all of the smart cards

belonging to the salespeople by, for example, obtaining the cooperation of G.

Specifically, A can request G to install a request for communication with O whenever a smart card interacts with G and found to have A as a user but not B as a user. All that G needs to do is modify the file that is executed when H logs in to communicate with G and direct the smart card to call O.

The word "loyalty" is nowhere to be found in the passage cited by the Examiner. At best, the passage cited by the Examiner describes allowing a gasoline provider G to install an application on a smartcard, and allowing a bank B to be a provider of credit for gas sales to employees of A. There is no mention of suggestion of any "loyalty application" on a client as in claim 59. Consequently, obviousness has not been established with respect to claim 59.

b. Obviousness has not been established, since the reason to modify Deo et al. with a "loyalty application" does not have any rational underpinning.

Obviousness has not been established, since the Examiner's proposed reason to modify Deo et al. with a "loyalty application" does not have any rational underpinning. Here, the Examiner alleges that one would have modified Deo et al. with a "loyalty application" to provide "access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card." One would not have modified Deo et al. with a "loyalty application" in order to provide "access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card" as alleged by the Examiner, since a loyalty application would not necessarily benefit from providing access control at higher hierarchical levels. Since the rationale that is used to modify Deo et al. does not have any rational underpinning, obviousness has not been established with respect to claim 59.

5. Dependent claim 60

Dependent claim 60 depends from dependent claims 58 and 59, and independent claim 39. Dependent claim 60 recites "wherein the first application can access only that cell group while the second application can access that cell group and additional cell groups."

- a. Obviousness has not been established, since all limitations are not taught or suggested by the cited art.*

Appellants submit that dependent claim 60 is patentable, since it depends from independent claim 39 and dependent claims 58 and 59, which are patentable for the reasons provided above. In addition, dependent claim 59 recites "wherein the first application can access only that cell group while the second application can access that cell group and additional cell groups." Neither Deo et al. nor Carlisle et al. teaches or suggests this feature. At pages 30-31 of the final Office Action, the Examiner relies on the passage at column 16, lines 66-67 to column 17, lines 1-19 of Carlisle et al. Column 16, lines 66-67 to column 17, lines 1-19 of Carlisle et al. state:

Cooperation Between Service Providers

It is quite possible for service providers to form cooperative alliances. Such alliances can specify various activities which are carried out in the smart cards whenever the smart card is accessed, or when the smart card is accessed by a particular user. The number of such possibilities is limitless, and the example below is merely illustrative.

Assume, for example, that company A employs traveling salespeople who frequently need to purchase gasoline. A is likely to contract with O to issue a smart card for each of the salespeople (Holders) and request O to install A as a service provider and G as the gasoline provider. Sometime later, A may reach an agreement with bank B as a Provider of credit for the salespeople. That service can be remotely installed into all of the smart cards

belonging to the salespeople by, for example, obtaining the cooperation of G.

Specifically, A can request G to install a request for communication with O whenever a smart card interacts with G and found to have A as a user but not B as a user. All that G needs to do is modify the file that is executed when H logs in to communicate with G and direct the smart card to call O.

The limitation "wherein the first application can access only that cell group while the second application can access that cell group and additional cell groups." is nowhere to be found in the passage cited by the Examiner. At best, the passage cited by the Examiner describes allowing a gasoline provider G to install an application on a smartcard, and allowing a bank B to be a provider of credit for gas sales to employees of A. Consequently, obviousness has not been established with respect to claim 60.

- b. *Obviousness has not been established, since the reason to modify Deo et al. with a "first application [that] can access only that cell group while the second application can access that cell group and additional cell groups" does not have any rational underpinning.*

Obviousness has not been established, since the reason to modify Deo et al. with a "first application [that] can access only that cell group while the second application can access that cell group and additional cell groups" does not have any rational underpinning. Here, the Examiner alleges that one would have modified Deo et al. with passwords or keys to provide "access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card". One would not have modified Deo et al. with a "first application [that] can access only that cell group while the second application can access that cell group and additional cell groups" in order to provide "access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card," because a "first application [that] can access only that cell group while the second application can access that cell group and additional cell groups" would not necessarily benefit from providing access control at higher hierarchical levels. Actually, the Examiner's proposed motivation to "restrict access" teaches away from a "first application [that] can access only that

cell group while the second application can access that cell group and additional cell groups," since the first and second applications are sharing information in a cell group and access is not restricted between the applications for that cell group. Thus, the Examiner's cited motivation actually teaches away from the modification proposed by the Examiner.

Since the rationale that is used to modify Deo et al. does not have any rational underpinning, obviousness has not been established with respect to claim 59.

c. Improper hindsight was used to reject claim 60 and other claims

The rejection of claim 60 and other claims is based on improper hindsight. As explained by MPEP 2142:

To reach a proper determination under 35 U.S.C. 103, the examiner must step backward in time and into the shoes worn by the hypothetical "person of ordinary skill in the art" when the invention was unknown and just before it was made. In view of all factual information, the examiner must then make a determination whether the claimed invention "as a whole" would have been obvious at that time to that person. Knowledge of applicant's disclosure must be put aside in reaching this determination, yet kept in mind in order to determine the "differences," conduct the search and evaluate the "subject matter as a whole" of the invention. The tendency to resort to "hindsight" based upon applicant's disclosure is often difficult to avoid due to the very nature of the examination process. However, impermissible hindsight must be avoided and the legal conclusion must be reached on the basis of the facts gleaned from the prior art.

Here, although the Examiner rejects dependent claim 60 as "obvious." In the obviousness rejection of claim 60, the Examiner alleges that the one skilled in the art would have taken the following steps:

- i) looked to Deo et al. and decided that Deo et al. should have a plurality of applications on a client when there is no teaching or suggestion of such a feature in Deo et al.; and then

ii) looked to Deo et al., and then decided to modify Deo et al. with passwords or keys, even though the purpose of a primary component in Deo et al.'s smart card would be defeated if keys or passwords are used, and even though Deo et al. does not indicate that there is anything wrong with Deo et al.'s system; and then

iii) added a "first application [that] is associated with a first party and the second application [that] is associated with a second party, and wherein the first party and the second party have an existing business relationship and agree to share data on the secure token according to agreed security controls" (as recited in dependent claim 58), when no such feature exists in either Deo et al. or Carlisle et al., to provide "access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card," even though an agreement to share security controls would not benefit from access control at higher hierarchical levels including subfolders and folders; and then

iv) added a "loyalty application" (as recited in dependent claim 59), when no such feature exists in either Deo et al. or Carlisle et al., to provide "access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card," even though a loyalty application would not benefit from access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers; and then

v) added a "first application [that] can access only that cell group while [a] second application can access that cell group and additional cell groups" (as recited in dependent claim 60) when no such feature exists in either Deo et al. or Carlisle et al., and even though a "first application [that] can access only that cell group while [a] second application can access that cell group and additional cell groups" would not benefit from, and would actually teach away from, access control at higher hierarchical levels.

Clearly, it would not have been "obvious" for the person of skill in the art to follow this sequence of events, unless one had had the benefit of Appellants' disclosure first. Consequently, the obviousness rejections of record are based on improper hindsight.

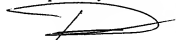
B. Rejection of claims 37 and 56 under 35 U.S.C. 103(a) as being obvious in view of Deo et al., Carlisle et al., and Brittenham et al.

As noted above, claims 37 and 56 may stand or fall with respect to independent claims 13 and 39. Appellants submit that the combination of Deo et al. and Carlisle et al. is improper for the reasons provided above.

8. CONCLUSION

In sum, there are many more reasons as to why the claims are patentable rather than unpatentable, and the rejections of record are simply improper. For the reasons provided above, it is respectfully submitted that the rejection should be reversed.

Respectfully submitted,



Patrick J. Jewik
Reg. No. 40,456

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 650-326-2400
Fax: 650-326-2422
61242373 v1

9. CLAIMS APPENDIX

Claims 1.-12. (Canceled).

Claim 13. A system for facilitating data management on a secure token, comprising:

- a client having a plurality of applications residing thereon; and
- a secure token having a storage architecture, wherein the storage architecture includes:
 - a directory and one or more attributes associated with the directory, wherein the one or more attributes associated with the directory are used to control access to the directory by the plurality of applications,
 - one or more cell groups under the directory, each cell group having one or more associated attributes, wherein the one or more attributes associated with a cell group are used to control access to that cell group by the plurality of applications, and
 - one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications, wherein the one or more attributes associated with a cell further control operations on contents of that cell by the plurality of applications, and
 - wherein the one or more attributes associated with the cell permit a first set of operations on the contents of that cell by a first application;
 - wherein the one or more attributes associated with the cell permit a second set of operations on the contents of that cell by a second application;
 - wherein the first set of operations is different from the second set of operations;

and

- wherein the one or more attributes associated with the directory, cell group, or cell are associated with a passcode or a key, wherein the client is adapted to use the passcode or key to access data in the directory, cell group, or cell.

Claims 14.-17. (Canceled).

Claim 18. A system for facilitating data management on a secure token,
comprising:
a client having a plurality of applications residing thereon; and
a secure token having a storage architecture, wherein the storage architecture
includes:

a directory and one or more attributes associated with the directory, wherein the
one or more attributes associated with the directory are used to control access to the directory by
the plurality of applications,

one or more cell groups under the directory, each cell group having one or more
associated attributes, wherein the one or more attributes associated with a cell group are used to
control access to that cell group by the plurality of applications, and

one or more cells under each cell group, each cell having one or more associated
attributes, wherein the one or more attributes associated with a cell are used to control access to
that cell by the plurality of applications, wherein the secure token is a smart card,

wherein the smart card is an open platform smart card, and

wherein the one or more attributes associated with the directory, cell group, or
cell are associated with a passcode or a key, wherein the client is adapted to use the passcode or
key to access data in the directory, cell group, or cell.

Claim 19. (Canceled).

Claim 20. A secure token comprising:

a directory and one or more attributes associated with the directory, wherein the
one or more attributes associated with the directory are used to control access to the directory by
a plurality of applications associated with a client,

one or more cell groups under the directory, each cell group having one or more
associated attributes, wherein the one or more attributes associated with a cell group are used to
control access to that cell group by the plurality of applications, and

one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications,

wherein the one or more attributes associated with the cell group permit a first application to access that cell group after a first access condition is satisfied;

wherein the one or more attributes associated with the cell group permit a second application to access that cell group after a second access condition is satisfied;

wherein the first access condition is different from the second access condition, and wherein the one or more attributes associated with the directory, cell group, or cell are associated with a passcode or a key, wherein the client is adapted to use the passcode or key to access data in the directory, cell group, or cell.

Claim 21. The secure token of claim 20 wherein the one or more attributes associated with the directory permit access to the directory by one application and deny access to the directory to another application.

Claim 22. (Canceled).

Claim 23. The secure token of claim 20 wherein the one or more attributes associated with the cell permit access to that cell by one application and deny access to that cell to another application.

Claim 24. The secure token of claim 20 wherein one or more additional cell groups are added to the directory subsequent to issuance of the secure token to a token holder.

Claim 25. The secure token of claim 20 wherein ownership of one of the one or more cell groups is determined subsequent to issuance of the secure token to a token holder.

Claim 26. The secure token of claim 20 wherein ownership of one of the one or more cell groups is modified subsequent to issuance of the secure token to a token holder.

Claim 27. The secure token of claim 20 wherein one or more additional cells are added to a cell group subsequent to issuance of the secure token to a token holder.

Claim 28. The secure token of claim 20
wherein the one or more attributes associated with the directory are modified in terms of permitting or denying access to the directory by the plurality of applications.

Claim 29. (Canceled).

Claim 30. The secure token of claim 20
wherein the one or more attributes associated with a cell are modified in terms of permitting or denying access to that cell by the plurality of applications.

Claim 31. The secure token of claim 20 wherein the one or more attributes associated with a cell further control operations on contents of that cell by the plurality of applications.

Claim 32. A secure token comprising:
a directory and one or more attributes associated with the directory, wherein the one or more attributes associated with the directory are used to control access to the directory by a plurality of applications associated with a client terminal,
one or more cell groups under the directory, each cell group having one or more associated attributes, wherein the one or more attributes associated with a cell group are used to control access to that cell group by the plurality of applications, and
one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications, wherein the one or more attributes associated with a cell further control operations on contents of that cell by the plurality of applications,
wherein the one or more attributes associated with the cell permit a first set of operations on the contents of that cell by a first application;

wherein the one or more attributes associated with the cell permit a second set of operations on the contents of that cell by a second application; and

wherein the first set of operations is different from the second set of operations,
and

wherein the one or more attributes associated with the directory, cell group, or cell are associated with a passcode or a key, wherein the client terminal is adapted to use the passcode or key to access data in the directory, cell group, or cell.

Claim 33. The secure token of claim 20 wherein the one or more attributes associated with the directory permit a first application to access the directory after a first access condition is satisfied;

wherein the one or more attributes associated with the directory permit a second application to access the directory after a second access condition is satisfied; and

wherein the first access condition is different from the second access condition.

Claim 34. (Canceled).

Claim 35. The secure token of claim 20 wherein the one or more attributes associated with the cell permit a first application to access that cell after a first access condition is satisfied;

wherein the one or more attributes associated with the cell permit a second application to access that cell after a second access condition is satisfied; and

wherein the first access condition is different from the second access condition.

Claim 36. . The secure token of claim 20 wherein the secure token is a smart card.

Claim 37. A secure token comprising:

a directory and one or more attributes associated with the directory, wherein the one or more attributes associated with the directory are used to control access to the directory by a plurality of applications associated with a client,

one or more cell groups under the directory, each cell group having one or more associated attributes, wherein the one or more attributes associated with a cell group are used to control access to that cell group by the plurality of applications, and

one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications, wherein the secure token is a smart card, and wherein the smart card is an open platform smart card,

wherein the one or more attributes associated with the directory, cell group, or cell are associated with a passcode or a key, wherein the client is adapted to use the passcode or key to access data in the directory, cell group, or cell.

Claim 38. The secure token of claim 36 wherein the smart card is a static or native smart card.

Claim 39. A method for facilitating data management on a secure token, comprising:

providing a directory and one or more attributes associated with the directory, wherein the one or more attributes associated with the directory are used to control access to the directory by a plurality of applications associated with a client,

providing one or more cell groups under the directory, each cell group having one or more associated attributes, wherein the one or more attributes associated with a cell group are used to control access to that cell group by the plurality of applications, and

providing one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications,

wherein the one or more attributes associated with the cell group permit a first application to access that cell group after a first access condition is satisfied;

wherein the one or more attributes associated with the cell group permit a second application to access that cell group after a second access condition is satisfied; and

wherein the first access condition is different from the second access condition,
and

wherein the one or more attributes associated with the directory, cell group, or cell are associated with a passcode or a key, wherein the client is adapted to use the passcode or key to access data in the directory, cell group, or cell.

Claim 40. The method of claim 39 wherein the one or more attributes associated with the directory permit access to the directory by one application and deny access to the directory to another application.

Claim 41. (Canceled).

Claim 42. The method of claim 39 wherein the one or more attributes associated with the cell permit access to that cell by one application and deny access to that cell to another application.

Claim 43. The method of claim 39 further comprising:
adding one or more additional cell groups to the directory subsequent to issuance of the secure token to a token holder.

Claim 44. The method of claim 39 further comprising:
determining ownership of one of the one or more cell groups subsequent to issuance of the secure token to a token holder.

Claim 45. The method of claim 39 further comprising:
modifying ownership of one of the one or more cell groups subsequent to issuance of the secure token to a token holder.

Claim 46. The method of claim 39 further comprising:
adding one or more additional cells to a cell group subsequent to issuance of the secure token to a token holder.

Claim 47. The method of claim 39 further comprising:
modifying the one or more attributes associated with the directory in terms of
permitting or denying access to the directory by the plurality of applications.

Claim 48. The method of claim 39 further comprising:
modifying the one or more attributes associated with a cell group in terms of
permitting or denying access to that cell group by the plurality of applications.

Claim 49. The method of claim 39 further comprising:
modifying the one or more attributes associated with a cell in terms of permitting
or denying access to that cell by the plurality of applications.

Claim 50. The method of claim 39 wherein the one or more attributes associated
with a cell further control operations on contents of that cell by the plurality of applications.

Claim 51. The method of claim 50 wherein the one or more attributes associated
with the cell permit a first set of operations on the contents of that cell by a first application;
wherein the one or more attributes associated with the cell permit a second set of
operations on the contents of that cell by a second application; and
wherein the first set of operations is different from the second set of operations.

Claim 52. The method of claim 39 wherein the one or more attributes associated
with the directory permit a first application to access the directory after a first access condition is
satisfied;
wherein the one or more attributes associated with the directory permit a second
application to access the directory after a second access condition is satisfied; and
wherein the first access condition is different from the second access condition.

Claim 53. (Canceled).

Claim 54. The method of claim 39 wherein the one or more attributes associated with the cell permit a first application to access that cell after a first access condition is satisfied; wherein the one or more attributes associated with the cell permit a second application to access that cell after a second access condition is satisfied; and wherein the first access condition is different from the second access condition.

Claim 55. The method of claim 39 wherein the secure token is a smart card.

Claim 56. A method for facilitating data management on a secure token, comprising:

providing a directory and one or more attributes associated with the directory, wherein the one or more attributes associated with the directory are used to control access to the directory by a plurality of applications associated with a client,

providing one or more cell groups under the directory, each cell group having one or more associated attributes, wherein the one or more attributes associated with a cell group are used to control access to that cell group by the plurality of applications, and

providing one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications, wherein the secured token is a smart card and wherein the smart card is an open platform smart card, and

wherein the one or more attributes associated with the directory, cell group, or cell are associated with a passcode or a key, wherein the client is adapted to use the passcode or key to access data in the directory, cell group, or cell.

Claim 57. The method of claim 55 wherein the smart card is a static or native smart card.

Claim 58. The method of claim 39 wherein the first application is associated with a first party and the second application is associated with a second party, and wherein the first

party and the second party have an existing business relationship and agree to share data on the secure token according to agreed security controls.

Claim 59. The method of claim 58 wherein the first application or the second application is a loyalty application.

Claim 60. The method of claim 59 wherein the first application can access only that cell group while the second application can access that cell group and additional cell groups.

Claim 61. The secure token of claim 32 wherein the first application is associated with a first party and the second application is associated with a second party, and wherein the first party and the second party have an existing business relationship and agree to share data on the secure token according to agreed security controls.

10. EVIDENCE APPENDIX

None.

Sonia Reed
Appl. No. 10/656,858
Page 35

PATENT
Attorney Docket No. 016222-012810US

11. RELATED PROCEEDINGS APPENDIX

None.